FINITENESS OF MINIMAL MODULAR SYMBOLS FOR SL_n

PAUL E. GUNNELLS

Abstract. Let $K/\mathbb{Q}$ be a number field with ring of integers $\mathscr{O}$, and let $\Gamma \subset SL_n(\mathscr{O})$ be a finite index subgroup. Using a classical construction from the geometry of numbers and the theory of modular symbols, we exhibit a finite spanning set of the highest nonvanishing rational cohomology group of Γ.

1. Introduction

Let $K/\mathbb{Q}$ be a number field with ring of integers $\mathscr{O}$. Let $\Gamma \subset SL_n(\mathscr{O})$ be a finite index subgroup, and let ν be the virtual cohomological dimension of Γ. That is, if $\Gamma' \subset \Gamma$ is any finite index torsion-free subgroup, then $H^i(\Gamma', M) = 0$ for $i > \nu$ and any $\mathbb{Z}\Gamma$-module M.

Let $\mathscr{M}$ be the free abelian group generated by the symbols $[v_1, \ldots, v_n]$, where the v_i are nonzero points in K^n, modulo the following relations:

(1) If τ is a permutation on n letters, then $[v_1, \ldots, v_n] = \operatorname{sgn}(\tau)[\tau(v_1), \ldots, \tau(v_n)]$, where $\operatorname{sgn}(\tau)$ is the sign of τ.
(2) If $q \in K^\times$, then $[qv_1, v_2, \ldots, v_n] = [v_1, \ldots, v_n]$.
(3) If the v_i are linearly dependent, then $[v_1, \ldots, v_n] = 0$.
(4) If $v_0, \ldots, v_n$ are nonzero points in K^n, then $\sum_i (-1)^i [v_0, \ldots, \hat{v}_i, \ldots, v_n] = 0$.

Elements of $\mathscr{M}$ are called *minimal modular symbols.* By a theorem of Ash [1] there is a surjective map of $\mathbb{Z}\Gamma$-modules

$$\mathscr{M} \longrightarrow H^\nu(\Gamma, \mathbb{Q}). \tag{5}$$

Hence $\mathscr{M}$ modulo Γ is a spanning set for $H^\nu(\Gamma, \mathbb{Q})$.

However, this spanning set is not finite. If $\mathscr{O}$ is a euclidean domain, Ash and Rudolph [2] define a subset $\mathscr{M}_u \subset \mathscr{M}$ with finite image under (5), and give an efficient algorithm to write any $[m] \in \mathscr{M}$ as a sum $[m] = \sum [m_i]$, where each $[m_i] \in \mathscr{M}_u$. Our goal in this note is more modest: in Theorem 2.5 we exhibit a *finite* spanning set for $H^\nu(\Gamma, \mathbb{Q})$ for all K, not necessarily euclidean, but we provide no practical

Date: December, 1997. Revised May, 1999.

1991 *Mathematics Subject Classification.* 11F75, 11H06.

Key words and phrases. Modular symbols, cohomology of arithmetic groups, geometry of numbers.

The author would like to thank Avner Ash, Farshid Hajir, and the referree for helpful comments. The author was partially supported by the NSF.

reduction algorithm. The proof relies on a classical construction of Minkowski from the geometry of numbers.

2. Statement of the result

2.1. Let $[K : \mathbb{Q}] = d$. For any ring R, let $M_n(R)$ be the $n \times n$ matrices over R.

Given $m \in M_n(\mathscr{O})$, let $[m] \in \mathscr{M}$ be the modular symbol $[m_1, \dots, m_n]$, where the m_i are the columns of m. The map $M_n(\mathscr{O}) \to \mathscr{M}$ is surjective, since using relations (1) and (2) we have $[v_1, \dots, v_n] = [q_1 v_1, \dots, q_n v_n]$ for any nonzero $v_i \in K^n$ and any $q_i \in K^\times$.

Let $N_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$ be the norm map. Define a map $\| \quad \| \colon M_n(K) \to \mathbb{Q}^{\geq 0}$ by

$$\|m\| = |N_{K/\mathbb{Q}}(\det m)|.$$

2.2. Let $C \geq 1$ be an integer, and define

$$M(C) := \left\{ m \in M_n(\mathscr{O}) \;\middle|\; \|m\| \leq C \right\}.$$

Let $\mathscr{M}(C) \subset \mathscr{M}$ be the set of modular symbols in the image of $M(C)$ under the map $M_n(\mathscr{O}) \to \mathscr{M}$.

2.3. Proposition. *Let $\Gamma \subset SL_n(\mathscr{O})$ be of finite index. Then for any $C \geq 1$, the set $\Gamma \backslash \mathscr{M}(C)$ is finite.*

Proof. It suffices to verify the statement for $\Gamma = SL_n(\mathscr{O})$. To simplify notation, we write G for $GL_n(\mathscr{O})$. If $m \in M_n(\mathscr{O})$, then we write $\Lambda(m)$ for the $\mathscr{O}$-lattice generated by the columns of m.

First, we claim that $G \backslash M(C)$ is finite for any $C \geq 1$. Indeed, the set

$$\left\{ m \;\middle|\; [\mathscr{O}^n : \Lambda(m)] \leq C \right\}$$

is finite modulo G. Now for any matrix m, the index $[\mathscr{O}^n : \Lambda(m)]$ is equal to $\mathscr{N}(\operatorname{ord}(T))$, where $\mathscr{N}$ denotes the ideal norm, and $\operatorname{ord}(T)$ is the *order ideal* of the torsion module $T := \mathscr{O}^n / \Lambda(m)$ ([3], §4D). Furthermore, $\operatorname{ord}(T)$ is a principal ideal generated by $\det(f)$, where $f \colon \mathscr{O}^n \to \mathscr{O}^n$ is any $\mathscr{O}$-linear endomorphism with image $\Lambda(m)$. Clearly for f we may take multiplication by m, and thus

$$\begin{aligned} [\mathscr{O}^n : \Lambda(m)] &= \mathscr{N}((\det m)) \\ &= |N_{K/\mathbb{Q}}(\det m)| \\ &= \|m\|. \end{aligned}$$

This implies $M(C)$ is finite modulo G.

We claim this implies $\mathscr{M}(C)$ is finite modulo Γ. To see this we use the following easily verified fact. Suppose a group A acts on a set S, and $B \lhd A$ is a normal subgroup. If A/B is a finite group, and $A \backslash S$ is finite, then $B \backslash S$ is finite.

To apply this, let $A = G$ and $B = Z \cdot \Gamma$, where Z is the center of G. The group $G/(Z \cdot \Gamma)$ is isomorphic to U/U^n, where $U = \mathscr{O}^\times$ and U^n is the subgroup of nth powers. Hence $G/(Z \cdot \Gamma)$ is finite by Dirichlet's unit theorem. Setting $S = M(C)$,

we have that $G\backslash M(C)$ finite implies that $(Z\cdot\Gamma)\backslash M(C)$ is finite. Since $M(C)$ maps surjectively onto $\mathscr{M}(C)$, and Z acts trivially on $\mathscr{M}$, the result follows. $\square$

2.4. Let $V = K\otimes\mathbb{R}\cong\mathbb{R}^r\times\mathbb{C}^s$, where $r+2s=d$. We define the *Minkowski constant*[1] M_K by

$$M_K = \left(\frac{\pi}{4}\right)^s \frac{d^d}{d!}.$$

We now state our main result.

2.5. Theorem. *The image of $\mathscr{M}(C)$ under* (5) *spans $H^\nu(\Gamma,\mathbb{Q})$ for*

$$C \geq \left\lfloor \left(\frac{\sqrt{|D_K|}}{M_K}\right)^n \right\rfloor.$$

3. Proof

3.1. Fix a modular symbol $[m]$, where $m\in M_n(\mathscr{O})$. We claim that if $\|m\| > (\sqrt{|D_K|}/M_K)^n$, then we can find a nonzero $x\in\mathscr{O}^n$ such that $x=\sum q_iv_i$ with $q_i\in K$ and $|N_{K/\mathbb{Q}}(q_i)|<1$. We may then use (4) to construct a relation $[m]=\sum(-1)^i[m_i]$, where

$$[m_i] := [v_1,\dots,v_{i-1},\hat{v}_i,x,v_{i+1},\dots,v_n].$$

Clearly $\|m_i\|<\|m\|$. This claim implies the theorem, because by iterating this process we can write any $[m]\in\mathscr{M}$ as a sum of symbols from $\mathscr{M}(C)$.

To prove the claim we use the *regular representation* of $\mathscr{O}$. Fix a $\mathbb{Z}$-basis $\omega_1 = 1,\omega_2,\dots,\omega_d$ of $\mathscr{O}$. Then this representation is the map $\mathscr{O}\to M_d(\mathbb{Z})$ defined by $\alpha\mapsto\ell_\alpha$, where ℓ_α is the matrix of the map $x\mapsto\alpha x$ in terms of the $\mathbb{Z}$-basis. This induces a ring homomorphism $\varphi\colon M_n(\mathscr{O})\to M_{nd}(\mathbb{Z})$, in which matrix entries are taken to $d\times d$ blocks. Via φ, any column vector $v\in\mathscr{O}^n$ determines d column vectors $\{v^1,\dots,v^d\}\subset\mathbb{Z}^{nd}$.

Now apply φ to m:

$$(v_1,\dots,v_n)\longmapsto(v_1^1,\dots,v_1^d,\dots,v_n^1,\dots,v_n^d)\in M_{nd}(\mathbb{Z}).$$

The matrix $\varphi(m_i)$ is obtained from $\varphi(m)$ by replacing the columns $v_i^1,\dots,v_i^d$ with $x^1,\dots,x^d$.

For $1\le i\le n$, $1\le j\le d$, let λ_i^j be real variables, and consider the region $S\subset\mathbb{R}^{nd}$ defined by

$$S := \left\{ \sum_{\substack{1\le i\le n\\ 1\le j\le d}} \lambda_i^j v_i^j \;\middle|\; \left|N_{K/\mathbb{Q}}\Bigl(\sum_j \lambda_i^j\omega_j\Bigr)\right| < 1, \text{where } 1\le i\le n \right\}.$$

[1] A classical result of Minkowski bounds the discriminant D_K of K: if $K\otimes\mathbb{R}\cong\mathbb{R}^r\times\mathbb{C}^s$, then $D_K^2\ge M_K$.

Here we interpret $N_{K/\mathbb{Q}}(\sum_j \lambda_i^j \omega_j)$ to mean the polynomial in $\mathbb{Z}[\lambda_i^j]$ constructed using the norm form.

3.2. Lemma. *Let $x \in \mathscr{O}$. Suppose that $x = \sum_i q_i v_i$, where $v_i \in \mathscr{O}$ and $q_i \in K$. Write $q_i = \sum_j q_i^j \omega_j$. Then $x^1 = \sum_{i,j} q_i^j v_i^j$.*

Proof. For any $x \in \mathscr{O}$, let $C_k(x)$ be the coefficient of ω_k in the expansion of x in terms of the fixed $\mathbb{Z}$-basis. By the definition of φ, the kth component of $x^j \in \mathbb{Z}^d$ is $C_k(\omega_j x)$. In particular, since $\omega_1 = 1$, the kth component of x^1 is $C_k(x) = C_k(\sum q_i v_i)$.

Now let $y \in \mathbb{Z}^d$ be the vector $\sum_{i,j} q_i^j v_i^j$. We will show that the components of y match those of x^1. Indeed, the kth component of y is $\sum_{i,j} q_i^j C_k(\omega_j v_i)$. But then

$$\begin{aligned} \sum_{i,j} q_i^j C_k(\omega_j v_i) &= \sum_{i,j} C_k(q_i^j \omega_j v_i) \\ &= C_k(\sum_{i,j} q_i^j \omega_j v_i) \\ &= C_k(\sum_i (\sum_j q_i^j \omega_j) v_i) \\ &= C_k(\sum_i q_i v_i). \end{aligned}$$

The final expression is the kth component of x^1, so the result follows. $\square$

3.3. Lemma. *There exists a nonzero $x \in \mathscr{O}^n$ such that $x = \sum q_i v_i$ with $q_i \in K$ and $|N_{K/\mathbb{Q}}(q_i)| < 1$ if and only if the region S contains a nonzero rational integral point.*

Proof. Let $x \in \mathscr{O}^n$ satisfy the hypotheses. Apply the regular representation to $x = \sum q_i v_i$ and Lemma 3.2 to each row of x. We find $x^1 = \sum q_i^j v_i^j$, where $q_i^j \in \mathbb{Q}$ and $q_i = \sum q_i^j \omega_j$. The condition $|N_{K/\mathbb{Q}}(q_i)| < 1$ is thus exactly $|N_{K/\mathbb{Q}}(\sum_j q_i^j \omega_j)| < 1$. Hence x^1 is a nonzero rational integral point in S. The converse follows by reversing this argument. $\square$

3.4. Now we will find a bounded symmetric convex body $P \subset S$ and show that if $\|m\| > (\sqrt{|D_K|}/M_K)^n$, then $\operatorname{vol} P > 2^{nd}$. Then by Minkowski's theorem ([4], IV.2.6) P and hence S will contain a nonzero integral point. By Lemma 3.3 this will imply Theorem 2.5.

To do this, apply $\varphi(m^{-1})$ to S. This carries $\{v_i^j\}$ onto the standard basis of $\mathbb{R}^{nd}$. We can then write $\varphi(m^{-1})(S)$ as the n-fold product T^n, where $T \subset \mathbb{R}^d$ is the region

$$T := \left\{ (y_1, \dots, y_d) \;\middle|\; \left| N_{K/\mathbb{Q}}\Big(\sum y_i \omega_i\Big) \right| \le 1 \right\}.$$

This region can be transformed further as follows. The vector space V contains $\mathscr{O}$, embedded by $\alpha \mapsto \alpha \otimes 1$. Let $\mu\colon \mathbb{R}^d \to \mathbb{R}^d$ be the linear map taking the standard

basis of $\mathbb{Z}^d$ to $\{\omega_1 \otimes 1, \ldots, \omega_d \otimes 1\}$. Then

$$\mu(T) = \left\{(x_1, \ldots, x_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; |x_1 \cdots x_r| z_1 \bar{z}_1 \cdots z_s \bar{z}_s < 1\right\}.$$

Now we construct the *generalized octahedron* of Minkowski. This will be a bounded, symmetric, convex body in $\mu(T)$. Take polar coordinates (ρ_i, θ_i) for the z_i, and let $V^+ \subset V$ be the subset

$$V^+ := \left\{(x_1, \ldots, x_r, \rho_1, \theta_1, \ldots, \rho_s, \theta_s) \;\middle|\; x_i \geq 0,\ \rho_i \geq 0, \text{ and } \theta_i = 0\right\}.$$

3.5. Definition. Given a point $p \in \mu(T) \cap V^+$, let $Q(p)$ be the subset of $\mu(T)$ constructed as follows:

1. Construct the tangent hyperplane to $\mu(T) \cap V^+$ at p.
2. Use this hyperplane and the bounding hyperplanes of V^+ to cut out a $(2r)$-simplex Δ in V^+.
3. Apply the motions $x_i \mapsto -x_i$ and $\theta_i \mapsto \theta_i + \beta$, $0 \leq \beta \leq 2\pi$ to Δ to sweep out $Q(p)$ (cf. Figure 1).

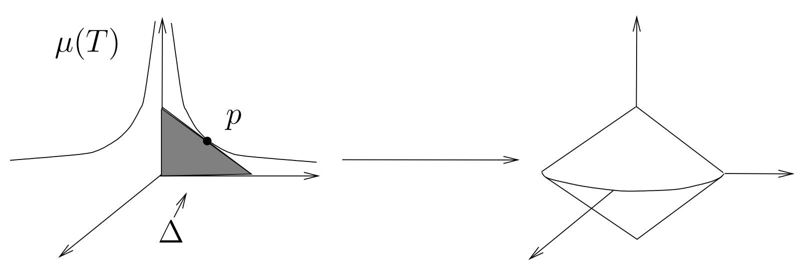

FIGURE 1. The generalized octahedron for $(r, s) = (1, 1)$.

3.6. Lemma. *$Q(p)$ is bounded, symmetric, and convex. The volume of $Q(p)$ is independent of p, and is*

$$2^{r+s} M_K. \tag{6}$$

Proof. All statements are standard results from the geometry of numbers ([4], IV.2), except for the independence of p. However, this is easy to verify. $\square$

3.7. We now complete the proof of the theorem. We choose $p \in \mu(T) \cap V^+$ and abbreviate $Q(p)$ to Q. Define $P \subset S$ by

$$P := \varphi(m)\big(\mu^{-1}Q \times \cdots \times \mu^{-1}Q\big).$$

P is symmetric, bounded, and convex, and

$$\operatorname{vol} P = |\det \varphi(m)| \left(\frac{\operatorname{vol} Q}{|\det \mu|}\right)^n. \tag{7}$$

Now in (7) we apply Lemma 3.6, and substitute $|\det \mu| = 2^{-s}\sqrt{|D_K|}$ and $\|m\| = |\det \varphi(m)|$. To ensure that $\operatorname{vol} P > 2^{nd}$, we require

$$\|m\| > \left(\frac{\sqrt{|D_K|}}{M_K}\right)^n,$$

as desired.

References

1. A. Ash, *A note on minimal modular symbols*, Proc. of the AMS **96** (1986), no. 3, 394–6.
2. A. Ash and L. Rudolph, *The modular symbol and continued fractions in higher dimensions*, Inv. math. **55** (1979), 241–250.
3. C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons, Inc., New York, 1981.
4. A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge University Press, Cambridge, 1993.

Department of Mathematics, Columbia University, New York, New York 10027
E-mail address: gunnells@math.columbia.edu